DISK-MATH

Simone Guggiari

Zusammenfassung 2015

⚠ some index might change (ZF 13)

2. Math reasoning, proofs and Logic

2.1 what is proof?

Def 2.1 A proof of statement S is a sequence of simple, easy verifable consecutive steps. Start from set of axioms (things postulated true) and known (previously proved) facts. Each step corresponds to the application of a derivation rule to a few already proven statements, resulting in a newly proved statement, until the final step proves S.

2.2 Propositions and Logical formulas

Def 2.2 A proposition [Aussage] is a mathem. statement that is TRUE or FALSE

Def 2.3 A true proposition is called theorem, lemma, corollary

Def 2.4 The logical values true/false have value 1/0

Def 2.5

NOT	negation	$\neg A$	(true if A false)
AND	conjunction	$A \wedge B$	(true if both A,B true)
OR	disjunction	$A \vee B$	(true if A or B or both true)

} logical operators on propositions

Def 2.6 formula (or propositional logic) is a correctly formed expression involving prop. symbols (A,B,C,...) and logical operators

implication, denoted $A \to B :\Leftrightarrow \neg A \vee B$ is a derived logical operator

two-sided implication $A \leftrightarrow B :\Leftrightarrow A \to B \wedge B \to A$

priority rules: $\neg$, $\wedge/\vee$, $\to/\leftrightarrow$ (stronger binding to weaker)

Def 2.7 $\top$ denotes the function that is constant true (1)
$\bot$ false (0)

Def 2.8 equivalent: two formulas F, G are called equivalent $F \Leftrightarrow G$, $F \equiv G$ if they correspond to the same function (table)

Def 2.9 tautology: a formula F (in prop. logic) is called tautology if it's true for all truth assignments of its prop. symbols

Def 2.10 satisfiable: a formula F is ~ [erfüllbar] if it is true for at least one truth assignment, unsatisfiable otherwise.

Lem 2.1 F is tautology iff $\neg F$ unsatisfiable

Def 2.11 $F \Rightarrow G$ means that $F \to G$ is a tautology (F implies G)

The 2.2 $\Rightarrow$ is transitive (if $F \Rightarrow G$ and $G \Rightarrow H$, $F \Rightarrow H$)

2.3 Quantifiers and Predicate Logic

Let's consider U as the universe in which we want to reason

Def 2.12 A k-ary predicate [Prädikat] P on U is a function $U^k \to \{0,1\}$

Def 2.13 For a universe U and pred. P(x) we define following logical statements:

$\forall x P(x)$	statement that P is true for all x
$\exists x P(x)$	" P is true for some $x \in U$ (one exists)

2.4 Some proof patterns and Techniques

The 2.3 If F and $F \to G$ are tautology, then G is T

Def 2.14 Direct proof of an implication $F \to G$: assume F and derive G from it, using proof steps

Def 2.15 Indirect proof $F \to G$: assume $\neg G$ and derive $\neg F$ (proving $G \vee \neg F$)

The 2.4 If $\neg F \to G$ and $\neg G$ are tautologies, then F is T

Def 2.16 Existence proof: $\exists x P(x)$

Def 2.17 inexistence " : $\neg\exists x P(x) :\Leftrightarrow \forall x \neg P(x)$

Def 2.18 Proof by counterexample: proof in the form $\neg\forall_x P(x)$ for some fixed predicate P, using $\exists x \neg P(x)$. the specific x is the counterexample

Proof by contradiction: $\neg F \to \bot$

Proof by contraposition: $F \Rightarrow G \wedge G \Rightarrow H$ then $F \Rightarrow H$ (transitivity)

case distinction: $F_1 \vee F_2 \vee \dots \vee F_k$ and $F_i \Rightarrow G$ for each i then G tautology

modus ponens: F T and $F \to G$, then G T

Proof by induction: it consists of 2 steps
1) basis step prove P(0)
2) induction step: prove $\forall n\,(P(n) \to P(n+1))$
assume P(n), derive P(n+1)

The 2.5 for every predicate P on $\mathbb{N}$ we have $P(0) \wedge \forall n(P(n) \to P(n+1)) \Rightarrow \forall n P(n)$

8. LOGIC

1. table for formula $\forall x \exists y\,(P(x,y) \wedge \neg P(y,x))$ $U^A = \mathbb{N}$ $P(a,b) = b > a$ (exists bigger $n \in \mathbb{N}$)

2. find all models for formula $(C \to (A \vee B)) \to (A \wedge B)$ simplify to $(C \wedge \neg A \wedge \neg B) \vee (A \wedge B)$
tutti i valori per cui è vero: far tabella
A ∧ B ⊂ C risolt

3. Sets, Relations, Functions

3.1 sets & operations on sets

Def 3.1 $A = B :\Leftrightarrow \forall x\,(x \in A \leftrightarrow x \in B)$

Def 3.2 cardinality of set, denoted $|A|$, is the # of its elements
a set can also be described by defining the properties of its elements
- If A is a set, and P is predicate defined on A, then $\{x \in A \mid P(x)\}$ denotes set of elements of A having property P.
- for the op. of forming ordered pairs of two obj, denoted (a,b) we have $(a,b) = (c,d) :\Leftrightarrow a = c \wedge b = d$

Def 3.3 subset (Teilmenge): A subset of B, $A \subseteq B$ if every element of A is also element of B ($A \subseteq B :\Leftrightarrow \forall x\,(x \in A \to x \in B)$)
two sets are equal $A = B \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$

⚠ $A \subseteq B$: what is inside A is found in B
$A \in B$: A is found inside B (as single element)

- in a set we dont care for double elements → elimina elementi uguali (sullo stesso livello)

Def 3.4 The empty set denoted $\emptyset$ or $\{\}$ is the set with no elements ($\forall x\, x \notin \emptyset$)
$P(\emptyset) = \{\emptyset\}$, cardinalità = 1 ↳ cardinalità 0

Lem 3.1 The empty set is subset of all sets $\forall A\,(\emptyset \subseteq A)$

Lem 3.2 " is unique

Def 3.5 The Power set of a set A, denoted $\mathcal{P}(A)$, is the set (made of sets) of all subsets of A: $\mathcal{P}(A) := \{S \mid S \subseteq A\}$ — contains $\emptyset$ aswell $\mathcal{P}(\emptyset) = \{\emptyset\}$
- has cardinality 2^k, $k = |A|$

Def 3.6 The union of 2 sets A and B defined as $A \cup B := \{x \mid x \in A \vee x \in B\}$
intersection $A \cap B :=$ "

→ let $\mathcal{A}$ be a set of sets. we define the union of all sets in $\mathcal{A}$ as the set of all x that are element of at least one set.
$\bigcup \mathcal{A} := \{x \mid \exists A \in \mathcal{A} : x \in A\}$
similarly we define the intersection on $\mathcal{A}$ as
$\bigcap \mathcal{A} := \{x \mid \forall A \in \mathcal{A} : x \in A\}$

Def 3.7 for a given universe U, the complement of a set A, denoted $\bar{A} := \{x \in U \mid x \notin A\}$

Def 3.8 the difference on sets B and A, denoted $B - A := \{x \in B \mid x \notin A\}$ (it's the complement of A, relative to B)

The 3.3 for any sets A, B, C and universe U, the following holds

$A \cap A = A$	$A \cup A = A$	independent
$A \cap B = B \cap A$	$A \cup B = B \cup A$	commutative
$A \cap (B \cap C) = (A \cap B) \cap C$	$A \cup (B \cup C) = (A \cup B) \cup C$	associative
$A \cap (A \cup B) = A$	$A \cup (A \cap B) = A$	absorption
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$		distributive
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$		
$A \cap \bar{A} = \emptyset$	$A \cup \bar{A} = U$	complementary
$A \subseteq B \Leftrightarrow A \cap B = A \wedge A \cup B = B$		consistency

Def 3.9 The cartesian product (made of pairs) $A \times B$ of 2 sets is the set of all ordered pairs with first component from A and the second from B. $A \times B := \{(a,b) \mid a \in A \wedge b \in B\}$ cardinality $|A| \cdot |B|$

→ more generally, the cart. product of sets $A_1, A_2, \dots, A_k$ is the set of all k-tuples with the i^{th} component from A_i:
$\bigtimes_{i=1}^{k} A_i := \{(a_1, \dots, a_k) \mid a_i \in A_i \text{ for } 1 \le i \le k\}$

3.2 Relations

Def 3.10 A (binary) relation ρ from set A to set B is a subset of $A \times B$.
if $A = B$, then ρ is called a relation on A.
instead of $(a,b) \in \rho$ one writes $a \rho b$

Def 3.11 For any set A, the identity relation on A, denoted $id = \{(a,a) \mid a \in A\}$

Def 3.12 the inverse of a relation ρ from A to B is the relation $\hat{\rho}$ from B to A such that: $a \rho b \Leftrightarrow b \hat{\rho} a$

Def 3.13 ρ relation $A \to B$, σ relation $B \to C$, then the composition of the 2, denoted $\rho\sigma$ (or $\rho \circ \sigma$) is the relation from $A \to C$ where
$a \rho\sigma c :\Leftrightarrow \exists b \in B : (a \rho b \wedge b \sigma c)$
→ the n-fold composition of ρ on A is denoted ρ^n

Lem 3.4 the composition of relations is associative $\rho(\sigma\phi) = (\rho\sigma)\phi$

Lem 3.5 ρ relation $A \to B$, σ rel $B \to C$. the inverse of $\rho\sigma$ $\widehat{\rho\sigma} := \hat{\sigma}\hat{\rho}$

→ a relation ρ on set A is called

Def 3.14	reflexive	if	$a \rho a$ $\forall a \in A$	$(id \subseteq \rho)$
.15	irreflexive	if	$a \not\rho a$ $\forall a \in A$	$(\rho \cap id = \emptyset)$
.16	symmetric	if	$a \rho b \Leftrightarrow b \rho a$	$(\rho = \hat{\rho})$
.17	antisymmetric	if	$a \rho b \wedge b \rho a \Rightarrow a = b$	$(\rho \cap \hat{\rho} \subseteq id)$
.18	transitive		$a \rho b \wedge b \rho c \Rightarrow a \rho c$	

⚠ it's not the opposite of symmetric

Lem 3.6 a relation ρ is transitive iff $\rho^2 \subseteq \rho$

Def 3.19 The transitive closure of ρ on A, denoted $\rho^* = \bigcup_{n=1}^{\infty} \rho^n$
example: $a R^* b \Leftrightarrow \exists a_1, \dots, a_n, \dots\ a R a_1 R a_2 \dots R b$

3.3 Equivalence relations

Def 3.20 an eq. rel is a relation that is reflexive, symmetric, transitive

Def 3.21 for an eq. rel θ on A and for $a \in A$, the set of elements that are equivalent to a according to θ is the equivalence class of a, $[a]_\theta := \{b \in A \mid b \theta a\}$

Lem 3.7 the intersection of 2 equiv. rel is an eq. relation.

Def 3.22 partition of a set A is a set $\{S_i \subseteq A\}$ of mutually disjoint subsets of A that covers A
$S_i \cap S_j = \emptyset$ and $\bigcup_i S_i = A$

Def 3.23 the set of equivalence classes of θ (eq. rel) on A, denoted $A/\theta := \{[a]_\theta \mid a \in A\}$ is the quotient set of A by θ (or simply A mod θ)

The 3.8 The set A/θ of eq. classes of θ on A is a partition of A

3.4 Partial order relations

Def 3.24 A partial order on a set A is a relation that is reflexive, antisymmetric, transitive. A set together with such relation $\le$ is called partially ordered set (poset) denoted $(A; \le)$
if the relation is not transitive, then it's a total order
→ we can define $<$ as $a < b \Leftrightarrow a \le b \wedge a \ne b$

Def 3.25 for a poset, 2 elements a, b are called comparable [vergleichbar] if $a \le b$ or $b \le a$, otherwise incomparable

Def 3.26 If any 2 elements are comparable, then A is totally ordered (or linearly ordered) by $\le$ (there is a relation between all)

Def 3.27 A poset is well-ordered [wohlgeordnet] if it's totally ordered and if every non empty subset of A has a least elem.

Def 3.28 In a poset, an element it's said to covers [überdecken] an element if $a < b$ and $\nexists c$ $a < c \wedge c < b$ (between). b is directly over

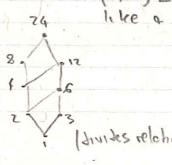
Def 3.29 The hasse diagram of a finite poset is the directed graph with the elements as vertices, and an edge $a \to b$ iff b covers a

$a \bullet \longrightarrow \bullet b$ $\quad b > a$

Usually drawn such that if b covers a ($b > a$) then b is drawn higher than a. In this case all arrows can be omitted (↑)

The 3.9 for posets $(A; \le)$, $(B; \sqsubseteq)$ the relation $\le$ defined on $A \times B$ $(a,b) \le (a_1, b_1) \Leftrightarrow a \le a_1 \wedge b \sqsubseteq b_1$ is also partial order

The 3.10 for same posets, $\le$ lex is defined
$(a,b) \le_{lex} (a_1, b_1) \Leftrightarrow a < a_1 \vee (a = a_1 \wedge b \sqsubseteq b_1)$
like a vocabulary



(divides relation)

Def 3.32 ▷ $(A,\leq)$ poset, $S \subseteq A$ subset. then

- $a \in S$ is minimal (maximal) elem of S if $\nexists b \in S : b < a$ $(b > a)$ (non ce ninuno freccia)
- $a \in S$ is least (greatest) elem of S if $\forall b \in S : a \leq b$ $(a \geq b)$ (la freccia tutti, vertice di tutti)
- $a \in A$ is lower (upper) bound [unter/obere Schranke] of S if $a \leq b$ $(a \geq b)$ $\forall b \in S$
- $a \in A$ is greatest lower bound (least upper bound) of S if a is the greatest (least) elem of the set of all lower (upper) bounds of S (vertice di tutti per tutti quelli non compresi (o uguali))

Def 3.33 $(A,\leq)$ poset. If a, b (the set $\{a,b\} \subseteq A$) have a greatest lower bound, it's called the meet of a,b $(a \wedge b)$; a least upp. B, then it's called join of a,b $(a \vee b)$

Def 3.34 A poset in which every pair of elem has meet and join is called a lattice [Verband]

3.5 Functions

Def 3.35 a funct $f: A \to B$ from a Domain [definitionsbereich] A to a codomain [Bildbereich, Wertbereich] B is a relation on $A \times B$, a subset $f \subseteq A \times B$ with special properties

1) $\forall a \in A \; \exists b \in B \; afb$ (f totally defined) ~ surj (each a maps to a single b)
2) $afb \wedge afb' \Rightarrow b = b'$ (f well defined) ~ inj

the set of all functions $A \to B$ is denoted B^A

Def 3.36 A partial funct is a relation on $A \times B$ such that condition 2 holds

Def 3.37 two functions are equal if they have same domain, codomain and are equal as relations
$f = g$ means, $\forall$ arguments f and g agree (including whether or not is defined)

Def 3.38 $f: A \to B$ and subset $S \subseteq A$, the image [Bild] of S under f is $f(S) := \{f(a) \mid a \in S\}$

Def 3.39 the subset $f(A)$ of B is called the image (range) $(\mathrm{Im}(f))$

Def 3.40 for subset $T \subseteq B$, the inverse image / preimage [Urbild] of T, denoted $f^{-1}(T)$, is the set of values in A that map to T.
$f^{-1}(T) := \{a \in A \mid f(a) \in T\}$

Def 3.41 $f: A \to B$ is called

- injective if $a \neq b \Rightarrow f(a) \neq f(b)$, no 2 distinct values mapped to same values (no collisions) each y has max one x
- surjective (or onto) if $\forall b, b = f(a)$ for some $a \in A$ (every value is reached) each y has min one x
- bijective, both inj & surj

Def 3.42 The composition of a function $f: A \to B$ and $g: B \to C$ denoted $g \circ f$ (or gf) is $g(f(a))$

Lem 3.11 Funct. composition is associative $(hg)f = h(gf)$

zz: $\exists$ meng $A : A \subseteq P(A) \wedge \exists$ meng $B : B \nsubseteq P(B)$ proof by example (existence): for set $A = \emptyset$, it holds $A \subseteq P(A)$. for $B = \{42\}$, $B \nsubseteq P(B)$, since $42 \notin \{\emptyset, \{42\}\}$

4. Combinatorics & Counting

4.1 Basic counting principles

- The cardinality of the union of n disjoint sets $A_1, \dots, A_n$ is equal to the sum of their cardinalities. This is the addition principle
  $\forall i,j, \; 1 \leq i < j \leq n : A_i \cap A_j = \emptyset \Rightarrow |A_1 \cup \dots \cup A_n| = \sum_{i=1}^{n} |A_i|$
- The multiplication principle (for finite sets) states that $|A \times B| = |A| \cdot |B|$ and, more generally, $|A_1 \times A_2 \times \dots \times A_n| = \prod_{i=1}^{n} |A_i|$ (they don't need to be disjoint)

Bijection principle: if $\exists$ bijection (one to one correspondence) between elements of A, B, then $|A| = |B|$

The 4.1 for $A_1, \dots, A_n$ finite sets, not disjoint

$$|A_1 \cup A_2 \dots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{i,j,k} |A_i \cap A_j \cap A_k| - \dots + (-1)^{n-1} |A_1 \cap A_2 \cap \dots \cap A_n|$$

The 4.2 consider only the first 2 terms

$$|A_1 \cup A_2 \dots \cup A_n| \geq \sum_{i=1}^{n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j|$$

Drawing k from n elements

	ordered	unordered
with repetit.	n^k	$\binom{n+k-1}{k}$
without rep	dispositions $\frac{n!}{(n-k)!}$	combinations $\binom{n}{k} := \frac{n!}{k!(n-k)!}$

$\binom{n}{k}$:= quanti modi ho di scegliere k elementi tra n

Consider the problem of counting a subset S of $A \times B$. We can count it in 2 ways: determining $\forall a$ the number m_a of $b \in B$ such that $(a,b) \in S$, or $\forall b$ n_b of $a \in A$. Then $|S| = \sum_{a \in A} m_a = \sum_{b \in B} n_b$ this is the double counting principle

The 4.3 If a set of n objects is partitioned into $k < n$ sets, then at least one of those sets contains $\lceil \frac{n}{k} \rceil$ objects. Pigeonhole principle

4.2 Binomial coefficients

$\binom{n}{0} = \binom{n}{n} = 1$

Lem 4.4 $\binom{n}{k} = \binom{n}{n-k}$

Lem 4.5 for $n > 0$, $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

The 4.6 for any (real or complex, $\mathbb{E}$) x, y and for every $n \geq 0$

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$ (pascal's triangle)

Cor 4.8 Let $k, m, n \in \mathbb{N}$, $m+n > 0$. Then $\binom{m+n}{k} = \sum_{i=0}^{k} \binom{m}{i}\binom{n}{k-i}$. in particular $\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2$ (vandermondes identity)

4.4 Countable and uncountable sets

Def 4.2

- Two sets A, B have same cardinality $A \sim B$ if $\exists$ a bijection $A \to B$
- $|B|$ is at least $|A|$, denoted $A \preceq B$, if $A \sim C$ for some $C \subseteq B$
- B dominates A, denoted $A \prec B$ if $A \preceq B \wedge A \not\sim B$
- A is countable [abzählbar] if $A \preceq \mathbb{N}$, uncountable [überabzählbar] otherwise

Lem 4.10

- the relation $\sim$ is an eq. relation (refl, symm, trans)
- $\preceq$ is transitive
- $A \subseteq B \Rightarrow A \preceq B$
- subset of countable set is also countable $A \subseteq B \wedge B \preceq \mathbb{N} \Rightarrow A \preceq \mathbb{N}$
- $A \preceq B \wedge B \preceq A \Rightarrow A \sim B$
- for 2 sets A, B exactly one holds: $A \prec B$, $A \sim B$, $A \succ B$

The 4.11 A set is countable iff it is finite or $A \sim \mathbb{N}$

The 4.12 The set $\{0,1\}^* = \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, \dots\}$ of finite binary sequences is countable (ε is the empty string)

The 4.13 the set $\mathbb{N} \times \mathbb{N} = (\mathbb{N}^2)$ of ordered pairs of nat. numbers is countable

The 4.14 the direct product of 2 countables sets is also countable
$A \preceq \mathbb{N} \wedge B \preceq \mathbb{N} \Rightarrow A \times B \preceq \mathbb{N}$

Cor 4.15 the rational numbers $\mathbb{Q}$ are countable ($\mathbb{Z} \sim \mathbb{N} \times \mathbb{N}$)

The 4.16 ▷ $A_1, A_2, \dots$ be countable sets

- $\forall n \in \mathbb{N}$, the set A^n of n-tuples over A is countable
- the union $A_1 \cup A_2 \cup \dots$ of a countable list of countable sets is countable
- The set A^* of finite countables sequence over A is countable

Def 4.3 Let $\{0,1\}^\infty$ denote the set of semi-infinite binary sequences

The 4.17 the set $\{0,1\}^\infty$ is uncountable

△ cantor's diagonalization argument.
contradiction, assume bijection with $\mathbb{N}$ exists.
$\beta_{i,j} = j^{th}$ bit in i^{th} sequence. $\bar{b}$ is complement of bit.
we define semi infinite seq $\alpha := \overline{\beta_{0,0}}, \overline{\beta_{1,1}}, \overline{\beta_{2,2}}, \dots \in \{0,1\}^\infty$ but $\nexists n \in \mathbb{N}$ with $\alpha = f(n)$ since α is built to disagree with at least 1 bit with every sequence. therefore no bijection exists.

Lem 4.18 if A uncountable and $A \preceq B$, then B uncountable. In particular, if a subset of B is uncountable, then so is B. (it has more elements)

Lem 4.20 If A uncount, B countable, $A - B$ uncountable $(\infty - n = \infty)$

The 4.21 The set $\mathbb{R}$ of real numbers is uncountable.

Lem 4.22 The interval $[0,1[$ in $\mathbb{R}$ is uncountable

$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$
$a^3 + b^3 = (a+b)(a^2 - ab + b^2)$

Cantor's theorem states that for any set A there is no surjective function $A \to P(A)$. with $A = \mathbb{N}$, this implies that $P(\mathbb{N})$ is not countable

zähler nenner

5. Graph Theory

5.2 Basic Concepts

Def 5.1 A (simple) graph $G = (V, \mathcal{E})$ consists of a finite set V of vertices [Knoten] and a set $\mathcal{E} \subseteq \{\{u,v\} \in V \mid u \neq v\}$ of edges [Kanten]
An edge $\{u,v\}$ is said to connect vertices u, v.
Vertices connected by edges are adjacent [benachbart] or neighbors

Def 5.2 The neighborhood of a vertex v is the set of vertices adjacent to v $\Gamma(v) := \{u \in V \mid \{u,v\} \in \mathcal{E}\}$.
The degree is the # of edges (or vertices) connected to it $:= |\Gamma(v)|$
A graph is k-regular if $\deg(v) = k \quad \forall v \in V$
undirected: it has $\frac{V(V-1)}{2}$ edges (max)

→ An important extension of this concept is when the edges are directed, eg they are ordered pairs (a,b) and not sets $\{a,b\}$.
u and v are called source and destination of edge.

Def 5.3 A directed graph $G = (V, \mathcal{E})$ consists of a finite set of Vertices and a set $\mathcal{E} \subseteq V \times V$ of directed edges

Def 5.4 The in-degree $\deg^-(v)$ of v is the # of edges entering v
out-degree $\deg^+(v)$ leaving v

Lem 5.1 In a directed graph $\sum_{v \in V} \deg^-(v) = \sum_{v \in V} \deg^+(v) = |\mathcal{E}|$
undirected " $\sum_{v \in V} \deg(v) = 2|\mathcal{E}|$

Def 5.5 A graph $G = (V, \mathcal{E})$ is a subgraph [Teilgraph] of a graph $H = (V', \mathcal{E}')$ denoted $G \subseteq H$ if $V \subseteq V' \wedge \mathcal{E} \subseteq \mathcal{E}'$

Def 5.6 The union of two Graphs G, H is $G \cup H := (V \cup V', \mathcal{E} \cup \mathcal{E}')$
The complement of G is $\overline{G} := (V, \overline{\mathcal{E}})$, with $\overline{\mathcal{E}}$ all edges non in $\mathcal{E}$

Def 5.7 G is bipartite if V can be split into 2 disjoint sets V_1, V_2 such that no edge connects 2 v in the same subset

Def 5.8 The adjacency matrix $A_G = [a_{ij}]$ of a directed/undir Graph G is the binary $n \times n$ matrix ($n = |V|$) where $a_{ij} = \begin{cases} 1 & \text{if } (v_i, v_j) \in \mathcal{E} \\ 0 & \text{otherwise} \end{cases}$
→ se elevo la matrice, $(\cdot)^k$ indica quanti percorsi di lunghezza k ci sono tra 2 vertici

Def 5.9 Two Graphs G, H are isomorphic, denoted $G \cong H$, if $\exists$ bijection $\pi : V \to V'$ such that renaming the vertices of V according to π results in H ($\{u,v\} \in \mathcal{E} \Leftrightarrow \{\pi(u), \pi(v)\} \in \mathcal{E}'$)
(for directed graphs, $\{u,v\}$ is (u,v))

Def 5.10 A graph G is contained in H denoted $G \preceq H$ if $\exists$ subgraph K of H that is isomorphic to G
$G \preceq H \Rightarrow \exists K \, (G \cong K \wedge K \subseteq H)$

The complete graph on n vertices, denoted K_n, is a simple graph with n vertices with any 2 vertices connected.
Its complement is the empty graph.
cardinality $\frac{n(n-1)}{2}$ (edges)

Def 5.11 a (m,n)-mesh [Gittergraph] is a graph $\Pi_{m,n}$ on $m \cdot n$ vertices with $V = \{(i,j) \mid 1 \le i \le m,\ 1 \le j \le n\}$ and where $(i,j),(i_1,j_1)$ are connected iff $i = i_1$ and $|j - j_1| = 1$ or $j = j_1$ and $|i - i_1| = 1$ (differs on one dx di 1)

Def 5.12 A path [Pfad] P_n consists of $n+1$ vertices connected like a chain (distinct)
$V = \{v_0, \dots, v_n\}$ $E = \{\{v_0, v_1\}, \{v_1, v_2\}, \dots\}$
directed path is same, but directed.

Def 5.13 A cycle [Kreis] C_n (for $n \ge 3$) are n vertices connected cyclically (a path with start v = end v)

Def 5.14 a d-dimensional hypercube is a graph on $V = \{0,1\}^d$ with $\{u,v\} \in E$ if u and v differ in exactly one bit. Q_d

Def 5.15 The complete bipartite graph $K_{m,n}$ has $m+n$ vertices, each in their partition, where every vertex in one partition is connected to all the vertex in the other.
$K_{m,n} = (V,E)$ with $V = B \cup W$, $B \cap W = \emptyset$, $|B| = m$, $|W| = n$ and $E = \{\{v,w\} \mid v \in B,\ w \in W\}$

$\Pi_{3,4}$ K_3 P_5 C_4 Q_4 $K_{4,3}$

Q_d is hamiltonian iff $d > 1$
$|V| = 2^d$ $|E| = 2|E|_{d-1} + |V|_{d-1}$

5.4 eulerians: since it's 3 regular (a cubo), it doesn't have an eulerians

5.3 Path and cycles

Def 5.16 a walk [Weg] from u to v of length n in a graph is a sequence $(v, v_1, \dots, v_{n-1}, v)$ of $n+1$ vertices such that consecutive vertices are connected.
If all vertices are distinct, it's a path
edges (but not vertex) are distinct, it's a tour
when start & end point are equal, path → cycle
(and length ≥ 3) tour → circuit [Schlaife]

Def 5.17 an undirected graph is connected [zusammenhängend] if any 2 vertices are connected by a path. The maximal connected subgraphs (the equivalence classes of the connected-ness relation) of a graph G are called the components of G

Def 5.18 A cycle in a graph is called Hamiltonian if it visits all vertices.
If it exists, the graph is called Hamiltonian. (no repetition of vertices)

Thm 5.2 A graph $G = (V,E)$ for which $|V| \ge 3$ and $\deg(u) + \deg(v) \ge |V|$ for every non adjacent pair (u,v) of vertices ($\{u,v\} \notin E$) is hamiltonian.
In particular, if $\deg(v) \ge |V|/2$ $\forall v \in V$, G is hamiltonian.
(due v qualsiasi ne hanno uno in comune)

Thm 5.3 Hypercube Q_d is hamiltonian for $d \ge 2$

Def 5.19 A hamiltonian cycle in hypercube is called gray code

5.4 Trees

Def 5.24 a tree is a undirected, connected graph with no cycles.
a forest is a undirected graph n (union of trees)
a leaf is a vertex with degree 1

Lem 5.6 a tree with $n \ge 2$ vertices has at least 2 leaves

Thm 5.7 for a graph $G = (V,E)$ with $n = |V|$, the following is equivalent
- G is a tree
- G has $n-1$ edges and no cycles
- G —"— and is connected

Def 5.26 a rooted tree is a tree with a distinguished vertex (root)
there is unique path from the root to every vertex v
Its length is the distance to the root
The height / depth of the sp. tree is the maximal distance of a leaf from the root.
The vertices on the path root-v are ancestors of v
The ancestor which is neighbour of v is called parent, and v child
A rooted tree is called d-ary if every vertex has at most d children.

Def 5.25 a spanning tree [Spannbaum] of connected Graph is subgraph of G (still a tree), and contains all vertices of G

5.5 Planar Graphs

Def 5.27 A graph is planar if it can be drawn with no edges crossing

Def 5.28 A drawing of a planar graph divides the plane into disjoint regions, one of which is infinite. The degree of a region is the # of edges that delimits its boundary. An edge is counted twice if it's a bridge (edge is bridge if when eliminated, graph is no more connected)

Thm 5.8 (Euler's formula) A plane drawing of a connected plane graph $G = (V,E)$ divides the plane into $r := |E| - |V| + 2$ regions
prove with spann. tree: eliminate 1 edge (thus 1 region) making the invariable $r - |E|$ constant... tree hanno $v = e + 1$, $r = 1$

Lem 5.9 for any connected plane graph G, the sum of the degrees of the regions is equal to $2|E|$ (each edge bounds 2 regions)

Thm 5.10 every connected planar graph G with $v \ge 3$ satisfies $|E| \le 3|V| - 6$
If G bipartite, then this stronger inequality holds: $|E| \le 2|V| - 4$
→ too many edges = no more planar

Cor 5.11 K_n is planar if $n \le 4$

Cor 5.12 $K_{3,3}$ is not planar

- we can define 3 operation on a graph
  1) delete edge
  2) deletion of singleton vertex
  3) merging neighboring vertices

Lem 5.13 If a sequence of these steps is performed on G and the resulting graph is still non planar, then G is non-planar
(you can't prove that it's planar this way since you can delete edges)

Def 5.30 A polyhedron is a solid bounded by finite # of polygon faces.
It is convex if all the points between 2 points in the polyhedron are also inside.

A polyhedron is regular for some $m,n \ge 3$ if every vertex meets exactly m faces and each face is a regular n-gon

Thm 5.16 There are exactly 5 regular polyhedra, with (m,n):

(3,3)	(3,4)	(4,3)	(3,5)	(5,3)
tetrahedron (4)	cube (hexahedron) (6)	octahedron (8)	dodecahedron (12)	icosahedron (20)

▷ $G = (V,E)$ graph that contains no triangle als subgrap. $\Leftrightarrow \forall \{u,v\}, \{v,w\} \in E : \deg(v) + \deg(v) \le |V|$ ▷ $u,v \in V$, $\{u,v\} \in E$. since G is free of triangles, u and v have no common neighbours. therefore $\Gamma(u) \cap \Gamma(v) = \emptyset$. It holds obviously $\Gamma(u) \cup \Gamma(v) \subseteq V$. with formula von cardinality of unions follows $|\Gamma(u) \cup \Gamma(v)| = |\Gamma(u)| + |\Gamma(v)| - |\Gamma(u) \cap \Gamma(v)| = \deg(u) + \deg(v)$ which is $\le |V|$

6. Number Theory

6.2 Divisors and division

Def 6.1 for $a,b \in \mathbb{Z}$, $a \neq 0$ we say a divides b, $a|b$, if it exists integer c such that $b = ac$. a is the divisor [Teiler] or factor, b is the multiple [Vielfaches] of a. The unique c is called quotient, and $c = b/a$. We write $a \nmid b$ if a doesn't divide b.

Thm 6.1 (Euclid) $\forall a,d \in \mathbb{Z}$, $d \neq 0$ $\exists$ unique $q,r \in \mathbb{Z}$ satisfying $a = dq + r$ $0 \le r < |d|$. a is dividend, d divisor, q is quotient, r remainder.
The remainder is denoted $R_d(a)$ or $a \bmod d$, $a \,\%\, d$.

Def 6.2 GCD for integers a,b, not both 0, an integer d is called a greatest common divisor of a and b if it divides both a and b, and if every common divisor of a and b divides d. ($d|a$, $d|b$ and $c|a$, $c|b \Rightarrow c|d$)

Def 6.3 for $a,b \in \mathbb{Z}$, not both 0, one denotes the unique positive great comm divisor by $\gcd(a,b)$ [ggT(a,b)] and calls it the gcd.
If $\gcd(a,b) = 1$, then a and b are called relatively prime [Teilfremd]
(they have no prime factors in common)

Def 6.4 for $a,b \in \mathbb{Z}$ the ideal generated by a and b [durch a und b erzeugtes Ideal], denoted $(a,b) := \{ua + vb \mid u,v \in \mathbb{Z}\}$ is a set.
Similarly, the ideal generated by a single integer is $(a) := \{va \mid v \in \mathbb{Z}\}$

Lem 6.2 for $a,b \in \mathbb{Z}$ $\exists d \mid (a,b) = (d)$

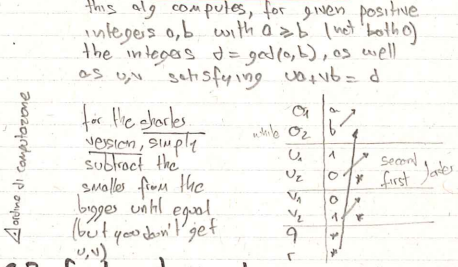
Lem 6.3 let $a,b \in \mathbb{Z}$ (not both 0). If $(a,b) = (d)$, then $d = \gcd(a,b)$

Cor 6.4 for $a,b \in \mathbb{Z}$ there exist $u,v \in \mathbb{Z}$ such that $\gcd(a,b) = ua + vb$

Thm 6.5 Extended-gcd-ALGORITHM (Euclid)
this alg computes, for given positive integers a,b with $a \ge b$ (not both 0) the integers $d = \gcd(a,b)$, as well as u,v satisfying $ua + vb = d$

```
o1 := a; o2 := b;
u1 := 1; u2 := 0;
v1 := 0; v2 := 1;
while (o2 > 0) {
    q := o1 div o2;   // quoziente senza resto
    r := o1 - q*o2;
    o1 := o2; o2 := r;
    t := u2; u2 := u1 - q*u2; u1 := t;
    t := v2; v2 := v1 - q*v2; v1 := t;
}
d := o1; u := u1; v := v1
```

for the checks version, simply subtract the smaller from the bigger until equal (but you don't get u,v)



6.3 Factorization into primes

Def 6.5 a positive integer $p > 1$ is called prime if its only positive divisors are 1 and p.
an integer > 1 not prime is called composite [zusammengesetzt]

Lem 6.6 If p is a prime that divides the product $x_1 \cdot x_2 \cdots x_n$ of integers, then p divides at least one of them ($p | x_i$ for some $i \in \{1 \dots n\}$)

Thm 6.7 Every positive integer can be written uniquely as the product of primes (up to the order in which factors are listed)

Thm 6.8 $\sqrt{n}$ is irrational unless n is a square ($n = c^2$ for some $c \in \mathbb{Z}$)

Def 6.6 The least common multiple (lcm) ℓ of 2 positive int a and b, denoted $\ell = \text{lcm}(a,b)$ is the common multiple of a,b which divides every common multiple of a,b ($a|\ell'$, $b|\ell'$, $\ell > 0$ and $a|\ell', b|\ell' \Rightarrow \ell|\ell'$)
△ $\gcd \cdot \text{lcm} = a \cdot b$

6.5 Congruences and Modular Arithmetic

Def 6.8 for $a,b,m \in \mathbb{Z}$ with $m \ge 1$ we say that a is congruent to b modulo m if m divides a-b. we write $a \equiv b \pmod m$ or simply $a \equiv_m b$ $\Leftrightarrow m | (a-b)$

Lem 6.13 for any $m \ge 1$, $\equiv_m$ is an equivalence relation on $\mathbb{Z}$ (refl, sym, trans)

Lem 6.14 If $a \equiv_m b$ and $c \equiv_m d$, then • $a + c \equiv_m b + d$ and • $ac \equiv_m bd$

Cor 6.15 Let $f(x_1 \dots x_k)$ be a multivariate polynomial in k variables with int coefficients and let $m \ge 1$. If $a_i \equiv_m b_i$ for $i \in \{1 \dots k\}$ then $f(a_1 \dots a_k) \equiv_m f(b_1 \dots b_k)$

→ There are m equivalence classes of the equiv. rel $\equiv_m$, namely $[0], [1], \dots, [m-1]$. (ogni numero appartiene ad uno di questi classi). Each eq. class $[a]$ has a natural representative $R_m(a) \in [a]$ in the set $\mathbb{Z}_m := \{0, 1, \dots, m-1\}$ of remainders modulo m.

Lem 6.16 for any $a,b,m \in \mathbb{Z}$ with $m \ge 1$
- $a \equiv_m R_m(a)$
- $a \equiv_m b \Leftrightarrow R_m(a) = R_m(b)$

Lem 6.17 —"—
- $R_m(a+b) = R_m(R_m(a) + R_m(b))$
- $R_m(ab) = R_m(R_m(a) \cdot R_m(b))$
- $R_m(a^b) = R_m(R_m(a)^b)$ (optional)

(modulo arithmetic)

Lem 6.18 the congruence equation $ax \equiv_m 1$ has a solution $x \in \mathbb{Z}_m$ if $\gcd(a,m) = 1$. (se non sono rel primi possiamo x va bene solo che stai assumendo multiplo di se stessa e non cambi niente). The solution is unique.

Def 6.9 If $\gcd(a,m) = 1$, the unique solution $x \in \mathbb{Z}_m$ to the congruence equation $ax \equiv_m 1$ is called the multiplicative inverse of a modulo m. One also uses the notation $x \equiv_m a^{-1}$ or $x \equiv_m 1/a$. (Use this to do division in $\mathbb{Z}_m$!
→ it can also be additive inverse

Thm 6.20 CRT (chinese remainder theorem)
let $m_1, m_2, \dots, m_r$ be pairwise relatively prime (you have to check it !!) and let $M := \prod_{i=1}^{r} m_i$. For every list $a_1, \dots, a_r$ with $0 \le a_i < m_i$ for each i, the system of congruence equations
$x \equiv_{m_1} a_1$, $x \equiv_{m_2} a_2$, $\dots$, $x \equiv_{m_r} a_r$
for x has a unique solution satisfying $0 \le x < \Pi$ (la soluz è unica solo in questo intervallo)
with $M_i := M/m_i$ and $N_i \equiv_{m_i} M_i^{-1}$ ($N_i M_i \equiv_{m_i} 1$)

$x = R_\Pi\left(\sum_{i=1}^{r} a_i M_i N_i\right)$

① compute Π, M_i;
② compute N_i;
③ compute $\sum \bmod \Pi$

6.6 The Diffie-Hellman key-agreement protocol

Alice: select x_A at random from $\{0,1,\dots p-2\}$; $Y_A := R_p(g^{x_A})$; $k_{AB} := R_p(Y_B^{x_A})$
Bob: select x_B at random from $\{0,1,\dots p-2\}$; $Y_B := R_p(g^{x_B})$; $k_{BA} := R_p(Y_A^{x_B})$
Y_A →, ← Y_B

p, g public parameters
analogy: padlock no key
public key cryptography – uses exponential mod of large prime
assymetry in computation difficulty = safety

#primi . 2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97,...

$a \overset{cz}{=} a*e \overset{cs}{=} a*(\hat{a}*\hat{\hat{a}}) \overset{as}{=} (a*\hat{a})*\hat{\hat{a}} \overset{cs}{=} e*\hat{\hat{a}} \overset{cz}{=} \hat{\hat{a}}$

$a*b \overset{s}{=} \hat{a}*\hat{b}*a = \hat{a}*b*((a*b)*(\hat{b}*\hat{a})) \overset{as}{=} (\hat{a}*b)*((a*b)*(\hat{b}*\hat{a})) \overset{s}{=} (\hat{a}*b)*(a*b)*(\hat{b}*\hat{a})$ assume $(a*b)*(\hat{b}*\hat{a}) = e$

$b \overset{z}{=} e*b \overset{s}{=} (\hat{a}*a)*b \overset{1}{=} \hat{a}*(a*b) \overset{\text{commutative}}{=} \hat{a}*(a*c) \overset{1}{=} (\hat{a}*a)*c \overset{3}{=} e*c \overset{z}{=} c$ $\quad e*(\hat{b}*\hat{a}) \overset{s}{=} \hat{b}*\hat{a}$

7. Algebra

7.1 Introduction

Def 7.1 an operation on a set S is a function $S^n \to S$, where $n \geq 1$ is called the "arity" of the operation

Def 7.2 An algebra (or algebraic system, Ω-algebra) is a pair $\langle S; \Omega \rangle$ where S is a set (the carrier [Trägermenge] of the algebra) and $\Omega = (\omega_1, \dots \omega_n)$ is a list of operations on S.

7.2 Semigroups, Monoids, Groups

Def 7.3 A left (right) neutral element (or identity element) of an algebra $\langle S, * \rangle$ is an element $e \in S$ such that $e*a = a$ ($a*e = a$) $\forall a \in S$.
If $e*a = a*e = a$, then e is simply called neutral element (NE)

Lem 7.1 If $\langle S, * \rangle$ has both a left and a right NE, then they are equal.
In particular, $\langle S, * \rangle$ can have at most one neutral element.

Def 7.4 A binary operation $*$ on a set S is associative if $a*(b*c) = (a*b)*c$ for all $a, b, c \in S$.

Def 7.5 A semigroup [Halbgruppe] is an algebra $\langle S, * \rangle$ where $*$ is associative

Def 7.6 A monoid (½) is an algebra $\langle M, *, e \rangle$ where $*$ is associat and e is the neutral element.
[A heterogeneous algebraic system is an algebra that can have multiple carrier sets]

Def 7.7 A left (right) inverse element of an element a in an algebra $\langle S, *, e \rangle$ is an element $b \in S$ such that $b*a = e$ ($a*b = e$).
If $b*a = a*b = e$, then b is simply called inverse of a.

Lem 7.2 In a monoid $\langle M, *, e \rangle$, if $a \in M$ has a right and left inverse, then they are equal. In particular, a has at most one inverse.

Def 7.8 A group is an algebra $\langle G, * \rangle$ satisfying the following axioms:
- G1 $*$ is associative
- G2 $\exists e$ (neutral) element such that $a*e = e*a = a$ $\forall a \in G$
- G3 $\forall a \in G$ $\exists \hat{a}$ (inverse element) such that $a*\hat{a} = \hat{a}*a = e$

Def 7.9 A group $\langle G, * \rangle$ (or monoid or semigroup) is called commutative or abelian if $a*b = b*a$ $\forall a, b \in G$

Lem 7.3 for a group $\langle G, *, \hat{}, e \rangle$ we have, $\forall a, b, c \in G$ (prove with direct proof)
1. $\hat{(\hat{a})} = a$
2. $\hat{a}*b = \hat{b}*\hat{a}$
3. left cancell. law $a*b = a*c \Rightarrow b = c$
4. right " $b*a = c*a \Rightarrow b = c$
5. the eq $a*x = b$ has unique solution for any a, b. so does $x*a = b$

7.3 Homomorphisms and Isomorphisms

Def 7.10 for two compatible algebras (if there is a one to one correspondence between op. with same arity) $\langle S, \Omega \rangle$ and $\langle S', \Omega' \rangle$, a function $\psi : S \to S'$ is called homomorphism from $\langle S, \Omega \rangle$ to $\langle S', \Omega' \rangle$ if for every $\omega \in \Omega$ and corresponding $\omega' \in \Omega'$ (of same arity)
$\psi(\omega(a_1, \dots, a_n)) = \omega'(\psi(a_1), \dots \psi(a_n))$ $\forall a_i \in S$

→ A mapping from group $\langle G, *, \hat{}, e \rangle$ to group $\langle G', *, \hat{}, e' \rangle$ is homomorphism if
- $\psi(e) = e'$
- $\psi(\hat{a}) = \widehat{\psi(a)}$ $\forall a$
- $\psi(a*b) = \psi(a) * \psi(b)$ $\forall a, b$

Def 7.11 a bijective homomorphism ψ from $\langle S, \Omega \rangle$ to $\langle S', \Omega' \rangle$ is called an isomorphism (and the two algebras isomorphic), denoted $\langle S, \Omega \rangle \cong \langle S', \Omega' \rangle$ if such an isomorphism exists.

7.4 The Structure of Groups

Def 7.12 The direct product of n groups $\langle G_1, *_1 \rangle, \dots \langle G_n, *_n \rangle$ is the algebra $\langle G_1 \times G_2 \times \dots \times G_n, * \rangle$ where the operation $*$ is component-wise:
$(a_1, \dots a_n) * (b_1, \dots b_n) = (a_1 *_1 b_1, \dots a_n *_n b_n)$

Lem 7.14 $\langle G_1 \times \dots \times G_n, * \rangle$ is a group where the neutral element and the inversion operation are component-wise in the respective groups

Def 7.13 A subset H of a group $\langle G, *, \hat{}, e \rangle$ is called a subgroup of G, denoted $H \leq G$, if $\langle H, *, \hat{}, e \rangle$ is a group, i.e if H is closed with respect to all operations:
- $a*b \in H$ $\forall a, b \in H$
- $e \in H$
- $\hat{a} \in H$ $\forall a \in H$

(ensure to be stable internally)

Def 7.14 let G be a group, $a \in G$.
The order [Ordnung] of a, denoted $\text{ord}(a)$ is the least $m \geq 1$ such that $a^m = e$ if such m exists. If it doesn't, $\text{ord}(a) = \infty$
(quante volte, operato con se stesso, ho bisogno di farlo per ottenere il ne)

Def 7.15 for a finite group G, the order of G is $|G| := \#$ elements

Lem 7.5 In a finite group G, every element has a finite order
→ If G is a group and $a \in G$ has finite order, then for any $m \in \mathbb{Z}$ we have $a^m = a^{\text{Rest}(m)}$ (chiamo la parte dell'ordine che si ripete e bbe)

Def 7.16 The smallest subgroup of a group G containing the elem $a \in G$ is called the group generated by a, denoted $\langle a \rangle := \{a^n \mid n \in \mathbb{Z}\}$

Def 7.17 A group $G = \langle g \rangle$ generated by an element $g \in G$ is called cyclic, and g is called generator of G.

The 7.6 A cyclic group of order n is isomorphic to $\langle \mathbb{Z}_n, \oplus \rangle$, with $\oplus$ being addition mod n. This group is abelian. (commutative)

The 7.8 Lagrange Let G be a finite group and let H be a subgroup of G. Then the order of H divides the order of G ($|H| \mid |G|$) → no proof (fundamental)

Cor 7.9 For a finite group G, the order of every element divides the group order
$\text{ord}(a) \mid |G|$ $\forall a \in G$

Cor 7.10 Let G be a finite group. then $a^{|G|} = e$ $\forall a \in G$

Cor 7.11 Every group of prime order is cyclic, and in such group every element except the neutral element is a generator

Def 7.19 $\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m \mid \gcd(a, m) = 1\}$ $\quad \mathbb{Z}_p^* = \{1, 2, \dots, p-1\} = \mathbb{Z}_p - \{0\}$

Def 7.20 The Euler function $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ is defined as the cardinality of $\mathbb{Z}_n^*$
$\varphi(m) := |\mathbb{Z}_m^*|$

Lem 7.12 if $m = \prod_{i=1}^{r} p_i^{e_i}$ (prodotto di primi, con molteplicità e) then $\varphi(m) = \prod_{i=1}^{r} (p_i - 1) p_i^{e_i - 1}$
$\varphi(n) = n \cdot \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$ → for all primes that divide p (multiplicity doesn't count)
es $36 = 2^2 \cdot 3^2$ $\quad \varphi(36) = 36 \cdot (1 - \frac{1}{2})(1 - \frac{1}{3})$
$\Rightarrow \mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$

The 7.13 $\langle \mathbb{Z}_m^*; \odot, ^{-1}, 1 \rangle$ is a group ($\odot$ = mult with mod)

Cor 7.14 (Fermat, Euler) $\forall m \geq 2$ and a with $\gcd(a, m) = 1$, $\boxed{a^{\varphi(m)} \equiv_m 1}$
In particular, $\forall p$ prime and a not divisible by p $\quad a^{p-1} \equiv_p 1$

The 7.15 The group $\mathbb{Z}_m^*$ is cyclic if $m = 2, m = 4$, $m = p^e$ or $m = 2p^e$, where p is odd prime and $e \geq 1$

The 7.17 ▷ G be some finite group (multiplicatively written) and $e \in \mathbb{Z}$ a given exponent relatively prime to $|G|$ ($\gcd(e, |G|) = 1$).
The unique e^{th} root of $y \in G$, namely $x \in G$ satisfying $x^e = y$, can be computed according to $x = y^d$, where d is the multiplicative inverse of e mod $|G|$ ($d \equiv_{|G|} e^{-1}$) → $x = \sqrt[e]{y} \Leftrightarrow y = x^e$
$x = y^d \mid de \equiv_{|G|} 1$

→ RSA

Alice		Bob
Generates primes p, q		
$n = p \cdot q$ $\quad f = (p-1)(q-1)$		plaintext $m \in \{1, \dots, n-1\}$
select e	n, e →	
$d \equiv_f e^{-1}$	y ←	ciphertext $y = R_n(m^e)$
$m = R_n(y^d)$		

this uses the groups $\mathbb{Z}_n^*$, with $n = p \cdot q$
$\varphi(n) = |\mathbb{Z}_n^*| = (p-1)(q-1)$

7.5 Rings and Fields

Def 7.21 A ring (1,5) $\langle R, +, -, 0, \cdot, 1 \rangle$ is an algebraic system for which
1. $\langle R, +, -, 0 \rangle$ is an abelian (commutative) group
2. $\langle R, \cdot, 1 \rangle$ is a monoid
3. right and left distrib. laws: $a(b+c) = ab + ac$ and $(b+c)a = ba + ca$ $\forall a, b, c \in R$

→ A ring is called commutative if multiplication is comm ($ab = ba$)

Lem 7.18 for any ring $\langle R, +, -, 0, \cdot, 1 \rangle$
1. $0a = a0 = 0$ $\quad \forall a \in R$
2. $(-a)b = -ab$
3. $(-a)(-b) = ab$

for finite field $GF(p^n)$ it is p

4. If R is non trivial (has more than 1 elem) then $1 \neq 0$

Def 7.22 The characteristic of a ring is the order of 1 in the additive group, but we define it 0 if the order of 1 is ∞.
es $\mathbb{Z}_m \to m$, $\mathbb{Z} \to \infty$ $\quad 0$

Def 7.23 ▷ R commutative ring. for $a, b \in R$ we say a divides b ($a \mid b$) if $\exists c \in R$ such that $ac = b$. a is divisor [Teiler] / factor of b, b is multiple [Vielfaches] of a.

Lem 7.19 In any commutative ring,
1. If $a \mid b$ and $b \mid c$, then $a \mid c$ (| is transitive)
2. If $a \mid b$, then $a \mid ba$ $\forall c$
3. If $a \mid b$ and $a \mid c$, then $a \mid (b+c)$

Def 7.24 Zerodivisor: an element $a \neq 0$ of comm. ring R is called zerodivisor
Nullteiler if $ab = 0$ for some $b \neq 0$ in R

Def 7.25 Unit: an element u of a ring R is called a unit [Einheit] if u is invertible, i.e $uv = vu = 1$ for some $v \in R$. ($v = u^{-1}$)
The set of units in R is denoted R^*

Lem 7.20 For a ring R, R^* is a multiplicative group (1 is NE, all invertible, associat

Def 7.26 an Integral Domain [Integritätsbereich] is a nontrivial comm. ring without zerodivisors: $ab = 0 \Rightarrow a = 0 \vee b = 0$

Lem 7.21 In an integral domain, if $a \mid b$ then c with $ac = b$ is unique (and is denoted $c = b/a$)

Def 7.27 A polynomial $a(x)$ over a ring R in the indeterminate x is a formal expression in the form $a(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0 = \sum_{i=0}^{d} a_i x^i$ for some $d \in \mathbb{N}$.
The degree of $a(x)$ $\deg(a(x))$ is the greatest i for which $a_i \neq 0$.
The special polynomial 0 (all $a_i = 0$) is defined to have $\deg := -\infty$.
Let $R[x]$ denote the set of polynomials over R. ($a_i \in R$)

The 7.22 $R[x]$ is a ring.

Lem 7.23 If D is an integral domain, then so is $D[x]$. The units of $D[x]$ are the constant polynomials which are units in D. ($D[x]^* = D^*$)

Def 7.28 A field [Körper] (2) $\langle F, +, -, 0, \cdot, ^{-1}, 1 \rangle$ is a nontrivial comm. ring F in which every nonzero element is a unit (is invertible), ie $F^* = F - \{0\}$

The 7.24 $\mathbb{Z}_p$ is a field if p prime
The 7.25 A field is an integral domain
The 7.26 A finite integral domain is a field

7.6 Polynomials over a Field

Def 7.29 A polynomial $a(x) \in F[x]$ is called monic [normiert, normest] if the leading coefficient is 1 (eg $x^2 + 2$)

Def 7.30 A polynomial $a(x) \in F[x]$ with degree ≥ 1 is called irreducible if it is divisible only by constant polynomials and by const. multiples of $a(x)$.
→ Check if it is by testing all monic irreducible pol with $\deg \leq d/2$

Def 7.31 For polynomials $a(x)$ and $b(x)$ in $F[x]$ (not both 0) a pol $d(x)$ is called a greatest common divisor of $a(x)$ and $b(x)$ if $d(x) \mid a(x)$ and $d(x) \mid b(x)$, and if every common divisor of a, b divides $d(x)$.
It is called the greatest comm. divisor the monic pol which divides $a(x)$ and $b(x)$, denoted $\gcd(a(x), b(x))$. (! non deve per forza venir diviso da tutti gli altri)

The 7.28 Let F be a field. For any $a(x)$ and $b(x) \neq 0$ in $F[x]$ there exist unique $q(x)$ (quotient) and $r(x)$ (remainder) such that $a(x) = b(x) \cdot q(x) + r(x)$ with $\deg(r) < \deg(b)$

Def 7.35 Let $a(x) \in R[x]$. an element $\alpha \in R$ for which $a(\alpha) = 0$ is called a root [Nullstelle, Wurzel] of $a(x)$

Lem 7.31 for a field F, $\alpha \in F$ is a root of $a(x)$ if $\boxed{(x - \alpha) \mid a(x)}$

Cor 7.32 A polynomial $a(x)$ of degree 2 or 3 over F is irreducible if it has no root (thm doesn't work with pol. of degree ≥ 4)

Def 7.36 If α is a root of $a(x)$, then its multiplicity (quante volte appare) is the highest power of $(x - a)$ that divides $a(x)$

The 7.33 For an integral domain D, a nonzero polynomial $a(x) \in D[x]$ of degree d has at most d roots, counting multiplicities

Lem 7.34 A polynomial $a(x) \in F[x]$ of degree d is uniquely determined by any $d+1$ values of $a(x)$, ie by $a(\alpha_1), \dots, a(\alpha_{d+1})$ for any distinct $\alpha_i \in F$
→ This polynomial is then given by
$\boxed{a(x) = \sum_{i=1}^{d+1} \beta_i u_i(x)}$ with $\beta_i := a(\alpha_i)$
$u_i(x) = \frac{(x - \alpha_1) \dots (x - \alpha_{i-1})(x - \alpha_{i+1}) \dots (x - \alpha_{d+1})}{(\alpha_i - \alpha_1) \dots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \dots}$

Lagrange interpolation formula

$\beta \cdot u(x) = a(x)$

mancano sempre l'α_i-esimo termine $(x - \alpha_i)$

7.7 Finite Fields

→ Let $R_{m(x)}(a(x))$ denote the unique remainder when $a(x)$ is divided by $m(x)$. The concept of congruence modulo $m(x)$ is like modulum.
for $a(x), b(x) \in F[x]$, $a(x) \equiv_{m(x)} b(x) \;:\Leftrightarrow\; m(x) \mid (a(x) - b(x))$

Lem 7.35 Congruence modulo $m(x)$ is an equivalence rel on $F[x]$, and each eq. class has an unique representative of $\deg < \deg(m(x))$

Def 7.37 Let $m(x)$ be pol of degree d over $F[x]$. Then
$F[x]_{m(x)} := \{ a(x) \in F[x] \mid \deg(a(x)) < d \}$ (tutti i pol congrado minore di m)

Lem 7.36 Let F be a field with q elements and $m(x)$ pol of degree d over F.
Then $|F[x]_{m(x)}| = q^d$

Lem 7.37 $F[x]_{m(x)}$ is a ring with respect to $\oplus$ and $\odot$ (addition and mult. modulo $m(x)$)

Lem 7.38 The congruence equation $a(x)\, b(x) \equiv_{m(x)} 1$, for a given $a(x)$, has solution $b(x) \in F[x]_{m(x)}$ if $\gcd(a(x), m(x)) = 1$. The solution is unique. In other words,
$F[x]^*_{m(x)} = \{ a(x) \in F[x]_{m(x)} \mid \gcd(a(x), m(x)) = 1 \}$

Thm 7.39 The ring $F[x]_{m(x)}$ is a field iff $m(x)$ irreducible. (called extension field of F)
→ $GF(2) := \mathbb{Z}_2$ $\quad GF(3)[x]_{x^3} :=$ pol di grado ≤ 2 con coefficienti $0,1,2$

7.8 Some applications of Finite Fields

Def 7.38 A (t,n) secret sharing scheme (t out of n needed to reconstruct) for a finite domain S is a method for sharing a secret value $s \in S$ among n parties $P_1, \dots, P_n$ such that any t of the parties can reconstruct s, but no $t-1$ (or fewer) parties have any info about s (nuclear code)

Thm 7.43 Let $n < q$ and let each party P_i be publicly assigned a unique element α_i of $GF(q)$. If $a_1, \dots, a_{t-1}$ are chosen uniformly at random from $GF(q)$ and each party P_i gets the share $a(\alpha_i)$, where the polynomial $a(x) \in GF(x)$ is defined as $a(x) := a_{t-1}x^{t-1} + \dots + a_1 x + s$, then this is a (t,n)-secret sharing code.

Def 7.39 The encoding function $\mathcal{E}$ of an error correcting code for some alphabet $\mathcal{A}$ takes k information symbols $a_0, \dots, a_{k-1} \in \mathcal{A}$ and encodes them into a list $[c_0, \dots, c_{n-1}]$ of $n > k$ symbols in $\mathcal{A}$ (the codeword)
$\mathcal{E}: \mathcal{A}^k \to \mathcal{A}^n : [a_0, \dots, a_{k-1}] \to \mathcal{E}(a_0, \dots, a_{k-1}) = [c_0, \dots, c_{n-1}]$

Def 7.40 An (n,k)-error correcting code (simply $(n-k)$ code) $\mathcal{C}$ over the alphabet $\mathcal{A}$ with $|\mathcal{A}| = q$ is a subset of cardinality q^k of $\mathcal{A}^n$.

Def 7.41 The Hamming distance between two codewords is the number of position at which the two codewords differ.

Def 7.42 The minimum distance of an error-correcting code C is the minimum of the Hamming distance between any 2 codewords.

Def 7.43 A decoding function D for an $(n-k)$-error correcting code is a function $D: \mathcal{A}^n \to \mathcal{A}^k$

Def 7.44 A code $\mathcal{C}$ can correct t errors if there exists a decoding function D such that when $[r_0, \dots, r_{n-1}]$ is obtained from an arbitrary codeword $[c_0, \dots, c_{n-1}]$ by changing at most arbitrary t positions, then $\mathcal{E}(D([r_0, \dots, r_{n-1}])) = [c_0, \dots, c_{n-1}]$

Thm 7.44 A code $\mathcal{C}$ with minimum distance d can correct t errors $\Leftrightarrow d \geq 2t+1$ $\quad (t \leq \lfloor (d-1)/2 \rfloor)$

Thm 7.45 ▷ $\mathcal{A} = GF(q)$ and $\alpha_0, \dots, \alpha_{n-1}$ be arbitrary distinct elements of $GF(q)$. Consider the encoding funct. $\mathcal{E}(a_0, \dots, a_{k-1}) = [a(\alpha_0), \dots, a(\alpha_{n-1})]$, where $a(x) := a_{k-1}x^{k-1} + \dots + a_1 x + a_0$. This code has minimum distance $n - k + 1$

Irreducible polynomes $\mathbb{Z}_2[x]$ deg=1: $1+x, x$ deg=2: $1+x+x^2$ deg=3: $1+x+x^3, 1+x^2+x^3$
deg=4: $1+x+x^4, 1+x+x^2+x^3+x^4, 1+x^3+x^4$ deg=5: $1+x^2+x^5, 1+x+x^3+x^4+x^5, 1+x^3+x^5, \dots$
$1+x+x^3+x^4+x^5, 1+x^2+x^3+x^4+x^5, 1+x+x^2+x^4+x^5$

$S = \{s, s\}^*$ $\quad T(v \in S) = 1 \Leftrightarrow v$ is identity (es $ssss$, ss)
we have 6 rules, es $v|sss|v \vdash_R v|s|v$, ctx. complete Π
$P = (\{1, \dots, 6\} \times \mathbb{N})^*$ where each pair (i,j) represent using rule i on position j of resulting string
$\phi: S \times P \to \{0,1\}$ $\quad \phi((w,p)) = 1$ if by applying rule after rule on resulting strings w_i, with $w_0 = w$ you get ε, otherwise (error-not possible or result $\neq \varepsilon$) $\phi(-) = 0$

8. Logic

8.1 Elementary Concepts in Logic

Let S be the set of (syntactic representations of) mathematical statements. Every statement $s \in S$ is either true or false. The function $\tau: S \to \{0,1\}$ assigning to each $s \in S$ its truth value $\tau(s)$ can be called the truth function. This function defines the meaning (semantics) of objects in S. Let P be the set of proofs, for ex. strings over some alphabet. A proof p for a statement s is relative to a verification function $\phi: S \times P \to \{0,1\}$ where $\phi(s,p) = 1$ means that the proof is accepted (by the funct. ϕ). This funct defines what is a proof for statements s.

Def 8.1 A proof system is a quadruple $\Pi = (S, P, \tau, \phi)$
Def 8.2 A proof syst is sound [Widerspruchsfrei] if no false statement has a proof, ie $\forall s \in S$ for which exists $p \in P$ with $\phi(s,p) = 1$, we have $\tau(s) = 1$
Def 8.3 A proof syst is complete [Vollständig] if every true statement has a proof, ie $\forall s \in S$ with $\tau(s) = 1$, there exists $p \in P$ | $\phi(s,p) = 1$
→ In addition one requires the function ϕ be efficiently computable, (for some notion of efficiency) and that every true statement has a reasonably short proof.

Def 8.4 The syntax (cosa per forza/cosa ha senso) of a logic defines an alphabet of allowed symbols and specifies which strings (over the alphabet) are syntactically correct formulas.

Def 8.5 A formula generally contains certain variable parts which are not determined (by the formula) and can take on values in certain domains. A particular choice of these variable parts is called a structure.

Def 8.6 A structure is suitable [passend] for a formula F if all variable elem of F are defined (ie. if it makes the formula true or false)
It is acceptable even if it defines more variable elem. than needed.

Def 8.7 The semantics (tra le cose che hanno senso, quali sono giuste) of a logic is a function $\mathcal{O}$ assigning to each formula F and a suitable structure $\mathcal{A}$ a truth value $\mathcal{O}(F, \mathcal{A}) = \{0,1\}$

Def 8.8 A suitable structure $\mathcal{A}$ for which a formula F is true is called a model for F, and one writes $\mathcal{A} \models F$. More generally, for a set Π of formulas, a suitable structure for which all formulas in Π are true, is called a model, denoted $\mathcal{A} \models \Pi$. Otherwise $\mathcal{A} \not\models \Pi$

Def 8.9 A formula F (or set Π of formulas) is called satisfiable [erfüllbar] if there exists at least one model for F (or Π), unsatisfiable otherwise (denoted $\bot$)

Def 8.10 A formula F is called tautology [Tautologie] or valid [gültig, allgemein gültig) denoted $\top$, if it is true for every suitable structure.

Def 8.11 A formula G is a logical consequence [logische Folgerung] of a formula F (or set Π) denoted $F \models G$ (or $\Pi \models$) if every suitable structure for F (or Π) and G which is a model of F (Π) is also a model of G

Def 8.12 Two formulas F and G are equivalent ($F \equiv G$, $F \Leftrightarrow G$) if every suitable structure for F, G yields the same truth value for both F and G
(ie each is a logical consequence of the other, $F \equiv G :\Leftrightarrow F \models G \wedge G \models F$)

8.2 Logical Calculi

Def 8.13 A derivation rule [Schlussregel] is a rule for deriving a formula from a set of formulas (called the precondition). We write $\{F_1, \dots F_k\} \vdash_R G$ if G can be derived from that set of formulas by rule R.

Def 8.14 A logical calculus [Kalkül] K is a finite set of derivation rules
$K := \{R_1, \dots, R_m\}$

Def 8.15 A derivation [Herleitung] of a formula G from a set Π of formulas in a calculus K is a finite sequence (of some length n) of applications of rules in K, leading to G.
More precisely, we have $\Pi_0 := \Pi$, $\Pi_i := \Pi_{i-1} \cup \{G_i\}$ for $i \in [1,n]$, where $N \vdash_{R_i} G_i$ for some $N \subseteq \Pi_{i-1}$ and $R_i \in K$, and where $G_n = G$. We write $\Pi \vdash_K G$ if such derivation exists for given Π, K.

Def 8.16 A derivation rule is correct if forevery set Π of formulas and every formula F, $\Pi \vdash_R F \Rightarrow \Pi \models F$

Def 8.17 A calculus K is sound [Widerspruchsfrei] or correct if for every set Π of formulas and every formula F, if F can be derived from Π then it is also a logical consequence. $\Pi \vdash_K F \Rightarrow \Pi \models F$
K is complete [vollständig] if for every Π and F, if F is a logical consequence of Π, then it can also be derived. $\Pi \models F \Rightarrow \Pi \vdash_K F$
→ One writes $\vdash_K F$ if F can be derived from the empty set of formulas.

Lem 8.1 If $F \vdash_K G$ for a sound calculus, then $\models (F \to G)$
$\models \times$ ($\times$ is true)

8.3 Propositional Logic (aussage logic)

Def 8.18 (Syntax) An atomic formula is of the form A_i with $i \in \mathbb{N}$ (can also use $A, B, C, \dots$). A formula is defined inductively: An atomic formula is also a formula, and if F, G formulas, then so are $\neg F$, $F \vee G$, $F \wedge G$.
→ A formula of the form $(F \wedge G)$ is called conjunction (and), $(F \vee G)$ disjunction (or)

Def 8.19 (Semantics) For a set Π of atomic formulas, a truth-assignment [Wahrheits Belegung] is a function $\mathcal{A}: \Pi \to \{0,1\}$.
▷ Π^* be the set of formulas built from atomic formulas in Π. We extend the domain of $\mathcal{A}$ to Π^*, as follows:
- $\mathcal{A}((F \wedge G)) = 1$ if and only if $\mathcal{A}(F) = 1$ and $\mathcal{A}(G) = 1$
- $\mathcal{A}((F \vee G)) = 1$ — " — $\mathcal{A}(F) = 1$ or $\mathcal{A}(G) = 1$
- $\mathcal{A}(\neg F) = 1$ — " — $\mathcal{A}(F) = 0$

Lem 8.2 (3) for any formulas F, G, H we have

1. $F \wedge F \equiv F$	$F \vee F \equiv F$	(independence)
2. $F \wedge G \equiv G \wedge F$	$F \vee G \equiv G \vee F$	(commutativity)
3. $(F \wedge G) \wedge H \equiv F \wedge (G \wedge H)$	$(F \vee G) \vee H \equiv F \vee (G \vee H)$	(associativity)
4. $F \wedge (F \vee G) \equiv F$	$F \vee (F \wedge G) \equiv F$	(absorption)
5. $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$		(distributive)
6. $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$		
7. $\neg\neg F \equiv F$		(double negation)
8. $\neg(F \wedge G) \equiv \neg F \vee \neg G$	$\neg(F \vee G) \equiv \neg F \wedge \neg G$	(de Morgan's rules)
9. $F \vee \top \equiv \top$	$F \wedge \top \equiv F$	(tautology rules)
10. $F \vee \bot \equiv F$	$F \wedge \bot \equiv \bot$	(unsatisfiability rules)
11. $F \vee \neg F \equiv \top$	$F \wedge \neg F \equiv \bot$	

Def 8.20 A literal is an atomic formula or the negation of an atomic formula
Def 8.21 A formula F is in CNF (conjunctive normal form) if it is a conjuction of disjunction of literals, ie. the form $F = (L_{11} \vee \dots \vee L_{1m_1}) \wedge \dots \wedge (L_{n1} \vee \dots \vee L_{nm_n})$ for some literals L_{ij} (or) and (or) (uses 0's)
Def 8.22 DND (disjunctive normal form) disjunction of conjunction of literals, $F = (L_{11} \wedge \dots \wedge L_{1m_1}) \vee \dots \vee (L_{n1} \wedge \dots \wedge L_{nm_n})$ (and) or (and) (my favourite (uses 1's)

The 8.3 Every formula is equivalent to a formula in CNF, and also one in DNF.
Def 8.23 A clause is a set of literals.
Def 8.24 The set of clauses associated to a formula F in CNF, denoted $K(F) := \{\{L_{11}, \dots, L_{1m_1}\}, \dots, \{L_{n1}, \dots, L_{nm_n}\}\}$.
The set of clauses associated to a set of formulas $\Pi = \{F_1, \dots, F_n\}$ is the union of their clause sets: $K(\Pi) := \bigcup_{i=1}^{n} K_i(F_i)$

Def 8.25 A clause K is a resolvent of clauses K_1 and K_2 if there is a literal l such that $l \in K_1$, $\neg l \in K_2$, and $K = (K_1 - \{l\}) \cup (K_2 - \{\neg l\})$
→ Given a set K of clauses, a resolution step takes two clauses $K_1, K_2 \in K$, computes the resolvent and adds it to K ~~(among K_1, K_2)~~ for consistency, one can write the resolution rule as $\{K_1, K_2\} \vdash_{res} K$.
The resolution calculus, denoted Res, consists of this single rule. $Res = \{\vdash_{res}\}$

Lem 8.4 The resolution calculus is sound/correct. (if $K \vdash_{res} \square$, then $K \models \square$)
The 8.5 A set Π of formulas is unsatisfiable iff $K(\Pi) \vdash_{res} \emptyset$.
(così provi che già il punto di partenza non era soddisfabile)

8.4 Predicate Logic

Def 8.26 (Syntax of predicate logic)
- a variable is of the form x_i, $i \in \mathbb{N}$
- a function symbol is of the form $f_i^{(k)}$, with $i, k \in \mathbb{N}$, where k denotes the # of arguments of the function. If $k = 0$, the funct. symbol is called const.
- a predicate symbol is of the form $P_i^{(k)}$ with $i, k \in \mathbb{N}$ (k is the # of arguments of the predicate)
- a term (ritorna un valore) is defined inductively: a variable is a term, and if $t_1, \dots, t_k$ are terms, then $f_i^{(k)}(t_1, \dots, t_k)$ is also a term.
- a formula (ritorna 0/1) is defined inductively:
  - if $t_1, \dots, t_k$ are terms, then $P_i^{(k)}(t_1, \dots, t_k)$ is a formula, called atomic
  - if F, G formulas, then $\neg F$, $F \vee G$, $F \wedge G$ also are
  - $\forall x: F$ and $\exists x: F$ are also formulas (quantifiers)

Def 8.27 every occurrence of a variable in a formula is either bound or free. If a variable x occurs in a (sub-) formula of the form $\forall x G$ or $\exists x G$, then it is bound, otherwise it is free. A formula is closed if it contains no free variables.
→ free variables are those that can be set by a suitable structure

Def 8.28 for a formula F, a variable x and a term t, $F[x/t]$ denotes the formula obtained from F by substituting every free occurrence of x by t.

Def 8.29 a structure is a tuple $\mathcal{A} = (U, \phi, \psi, \xi)$ where
- U is a non-empty set, the UNIVERSE
- ϕ is a function assigning to each function symbol (in a certain subset of all funct. symbols) a function, where for a k-ary funct. symbol f, $\phi(f)$ is a funct $U^k \to U$
- ψ is a function assigning to each predicate symbol a function, where for a k-ary predicate symbol P, $\psi(P)$ is a function $U^k \to \{0,1\}$
- ξ is a function assigning to each variable symbol a value in U.

Def 8.30 (semantics) for a structure $\mathcal{A} = (U, \phi, \psi, \xi)$, we define the value of terms and the truth value of formulas under that structure.
- The value $\mathcal{A}(t)$ for a term t is defined as follows:
  - if t is a variable, then $\mathcal{A}(t) = \xi(t)$
  - if t is a function, of the form $f(t_1, \dots t_k)$ for t_i terms and a k-ary funct. symbol f, then $\mathcal{A}(t) = \phi(f)(\mathcal{A}(t_1), \dots, \mathcal{A}(t_k))$
- The truth value of a formula F is defined as follows:
  - $\mathcal{A}((F \wedge G)) = 1$ if and only if $\mathcal{A}(F) = 1$ and $\mathcal{A}(G) = 1$
  - $\mathcal{A}((F \vee G)) = 1$ — " — or
  - $\mathcal{A}(\neg F) = 1$ — " — $\mathcal{A}(F) = 0$
  - if F is a predicate symbol of the form $F = P(t_1, \dots, t_k)$ for t_i terms and a k-ary predicate symbol P, then $\mathcal{A}(F) = \psi(P)(\mathcal{A}(t_1), \dots, \mathcal{A}(t_k))$
  - if F is of the form $\forall x G$ or $\exists x G$, then let $\mathcal{A}_{[x \to u]}$ be the same structure as $\mathcal{A}$, except that $\xi(x)$ is overwritten by u ($\xi(x) = u$)

$$\mathcal{A}(\forall x G) = \begin{cases} 1 & \text{if } \mathcal{A}_{[x\to u]}(G) = 1 \text{ for all } u \in U \\ 0 & \text{else} \end{cases}$$

$$\mathcal{A}(\exists x G) = \begin{cases} 1 & \text{if } \mathcal{A}_{[x\to u]}(G) = 1 \text{ for some } u \in U \\ 0 & \text{else} \end{cases}$$

Lem 8.6 Any equivalence that holds in propositional logic also holds in predicate logic. Moreover, for F, G, H formulas where H doesn't contain variable x, we have

1.	$\neg(\forall x F) \equiv \exists x \neg F$	2. $\neg(\exists x F) \equiv \forall x \neg F$
3.	$(\forall x F) \wedge (\forall x G) \equiv \forall x (F \wedge G)$	4. $(\exists x F) \vee (\exists x G) \equiv \exists x (F \vee G)$
5.	$\forall x \forall y F \equiv \forall y \forall x F$	6. $\exists x \exists y F \equiv \exists y \exists x F$
7.	$(\forall x F) \wedge H \equiv \forall x (F \wedge H)$	8. $(\forall x F) \vee H \equiv \forall x (F \vee H)$
9.	$(\exists x F) \wedge H \equiv \exists x (F \wedge H)$	10. $(\exists x F) \vee H \equiv \exists x (F \vee H)$

(point 7-10 hold since H doesn't depend on x)

- attention with 3 & 4, since changing $\wedge$ and $\vee$ respectively makes them not true

Lem 8.7 If one replaces a subformula G of a formula F by an equivalent (to G) formula H, then the resulting formula is equivalent to F

Lem 8.8 for a formula G in which x occurs only free and in which y doesn't occur,

$\forall x G \equiv \forall y G[x/y]$ and $\exists x G \equiv \exists y G[x/y]$

→ By appropriately renaming quantified variables one can transform any formula into an equivalent formula in which no variable appears both as bound and free, and such that all variables appearing after the quantifiers are distinct.

Such a formula is said to be in rectified [bereinigt] form.

Def 8.31 A formula of the form $Q_{x_1} Q_{x_2} \dots Q_{x_n} G$, where Q_i are arbitrary quantifiers ($\forall$ or $\exists$) and G is a formula free of quantifiers, is said to be in prenex form [Pränexform]

The 8.9 (theorema del barbiere ella) $\neg\exists x \forall y (P(y,x) \leftrightarrow \neg P(y,y))$
this is a tautology (law for every structure)
prove it by bringing the $\neg$ inside. ($\forall x \exists y (P(y,x) \leftrightarrow P(y,y))$ and setting $y = x$

Cor 8.10 (Russel's paradox) there exists no set that contains all sets S that do not contain themselves (ie $\{S \mid S \notin S\}$ is not a set)

Cor 8.11 The set $\{0,1\}^\infty$ is not countable

Cor 8.12 There are functions $\mathbb{N} \to \{0,1\}$ that are not computed by any program.

Esercizi 3. SETS, RELATIONS, FUNCTIONS

1. $\forall\forall$ $A \subseteq B \Leftrightarrow P(A) \subseteq P(B)$. show both directions: $A \subseteq B \Rightarrow P(A) \subseteq P(B)$: ▷ $A \subseteq B$: we need to show $\forall$ elem $S \in P(A)$, S also $\in P(B)$. ▷ S belieby elem of $P(A)$. from def 3.5 follows that $S \subseteq A$. from assumption $A \subseteq B$ and transitivity of $\subseteq$ it follows $S \subseteq B$. therefore $S \in P(B)$. since this holds $\forall S \in P(A)$, $P(A) \subseteq P(B)$. | $P(A) \subseteq P(B) \Rightarrow A \subseteq B$. ▷ $P(A) \subseteq P(B)$. since $A \in P(A)$ and $P(A) \subseteq P(B)$, $A \in P(B)$. therefore is $A \subseteq B$
2. for which sets A follows $A \times B = A \times C \Rightarrow B = C$. This holds $\forall$ sets $A \neq \emptyset$. If $A = \emptyset$, it follows $\forall B, C$: $A \times B = \emptyset \times B = \emptyset = \emptyset \times C = A \times C$. Let's show $B \subseteq C$. ▷ $b \in B$. from Def 3.9 follows that any $a \in A$ (exists since $A \neq \emptyset$) → that $(a,b) \in A \times B = A \times C$. from def 3.9 follows $b \in C$. To show $C \subseteq B$, do the same inverted. Therefore $B = C$
3. sets $A := \mathbb{R}^2$: $(x,y) \sim (x',y') \Leftrightarrow x^2+y^2 = x'^2+y'^2$. $\forall\forall$: $\sim$ eq. relation. show that it has following properties: reflexivity: easy, symmetry easy, transitivity: take 3 points. show it holds. explain the geometric meaning: the equivalence class $[(x,y)]$ contains all points distant $\sqrt{x^2+y^2}$ from origin. this is the circle with center O and that radius. es: eq. class $[(0,0)]$ is simply the point $(0,0)$
4. $\forall\forall$ or widerlegen: $\forall$ partial order $\leq$, the rel. $<\; := \leq \wedge \neq$ is transitive. Yes, it is. To show: $\forall x \forall y \forall z \; (x \leq y \wedge x \neq y \wedge y \leq z \wedge y \neq z) \to (x \leq z \wedge x \neq z)$. from $(x \leq y \wedge y \leq z)$ and transitivity of $\leq$ follows $(x \leq z)$. But generally from $x \neq y$, $y \neq z$ it doesn't follow $x \neq z$. To prove this, use contradiction: assume the upheaton doesn't hold. therefore $\exists x \exists y \exists z (x \leq y \wedge x \neq y \wedge y \leq z \wedge y \neq z \wedge x = z)$. but from this it follows $x \leq y \wedge y \leq x$. from this and asymmetry of $\leq$ follows $x = y$, which contradicts $x \neq y$
5. ▷ $\lesssim$ reflexive and transitive relation. ▷ $\sim$ relation on: $a \sim b \Leftrightarrow a \lesssim b \wedge b \lesssim a$. without proving that $\sim$ is eq. relation, lets define relation $\leq$ on $A/\sim$ of equivalence class with $[a] \leq [b] \Leftrightarrow \forall x \in [a] \; \forall y \in [b] \; x \lesssim y$. a) $\forall\forall$ $a, b \in A$: $[a] \leq [b] \Leftrightarrow a \lesssim b$ Lets show both directions "⇒": Let $[a] \leq [b]$, d.h. $\forall x \in [a], \forall y \in [b] \; x \lesssim y$. since $a \in [a]$ and $b \in [b]$, $x \lesssim y$ holds for $x = a$, $y = b$. therefore $a \lesssim b$. "⇐" assume $a \lesssim b$ holds. ▷ $x \in [a]$, $y \in [b]$. from definition of eq. classe, it means $x \sim a$, $y \sim b$. from def of $\sim$ it follows $x \lesssim a$, $b \lesssim y$. Together with $a \lesssim b$ and transitivity of $\lesssim$ it follows $x \lesssim y$. Since x, y were belieby (any), follows $\forall x \in [a], \forall y \in [b]$ $x \lesssim y$, also $[a] \leq [b]$. b) $\forall\forall$ $\leq$ partial order on $A/\sim$. you need to show that $\leq$ has following properties: reflexivity: ▷ $a \in A$. since $\lesssim$ reflexive, $a \lesssim a$. with aufgabe a) follows $[a] \leq [a]$ symmetry: assume $[a] \leq [b]$, $[b] \leq [a]$. from point a) follows $a \lesssim b$, $b \lesssim a$. from def of $\sim$ follows $a \sim b$. With Theorem 3.9 follows $[a] = [b]$. transitivity: assuming $[a] \leq [b]$ and $[b] \leq [c]$, from point a) follows $a \lesssim b$, $b \lesssim c$. with transitivity follows (of $\lesssim$) $a \lesssim c$. from a) follows $[a] \leq [c]$.

4. COMBINATORICS & COUNTING

1. In how many ways can you distribute 20 identical balls in 4 distinguishable boxes, so that each box doesn't remain empty ★ ★ ★ ★ |★★★★★★★|★★★★★★★|★

you can think of a row of 20 stars, to divide, and each of the 4 can't be empty. ▷ A set of vertical lines between stars, but no left or right (respect conditions). there are 19 places to set 3 divisions. therefore $|A| = |B| = \binom{19}{3} = 969$
2. In how many ways can you paint a cube using 6 colors? Let M the set of searched colorations ▷ A set of colorations of a cube, R the set of all rotations. Each coloration A corresponds to one rotation M and a rotation R. therefore $A = M \times R \Rightarrow |M| = \frac{|A|}{|R|} = \frac{6!}{24} = 30$ // (6! colorations, 6.4 rotations)
3. In a test there are 7 exercises. each exercise is correctly solved by 75 students. each students solves correctly exactly 3 exercises. How many students take the test?
$7 \cdot 78 / 3 = 182$ students

5. GRAPH THEORY

1. How many circles of length r contains K_n. We consider the # of circles with r nodes, and all the permutations these can have. from a circle C_r we can build $r.2$ tuples. To each tuple we assign a circle. Therefore there are $r.2$ times more tuples than circles. There are $D\binom{n}{k} = \frac{n!}{(n-k)!}$ possibilities to build a tuple, therefore we have $\frac{n!}{(n-r)!} \cdot \frac{1}{2r}$
2. for which $a, b \geq 2$ contains mesh _____ $\Pi_{a,b}$ a Hamiltonkreis? Let's distinguish 2 cases: a oder b even: we always have a Hamiltonkreis: where the floor of the comb goes on a direction with even # of nodes (formal proof: use induction: 1^{st} $a = 2$, $a \to a+2$. If both a, b odd: note each mesh $\Pi_{a,b}$ can be painted with 2 colors. therefore, so does every subgraph. The circle would contain odd # of nodes, alternating colors. Thus is impossible (# nodes odd)
3. Prove: $\forall$ planar connected graph $G = (V, \mathcal{E})$ with $|V| \geq 3$: $\sum_{v \in V} \deg(V) \leq 6|V| - 12$. from lemma 5.1 $\sum \deg(v) = 2|\mathcal{E}|$. from th 5.8: $|\mathcal{E}| \leq 3|V| - 6$. therefore $\sum \deg(V) = 2|\mathcal{E}| \leq 6|V| - 12$
4. ▷ G graph, A_G its adjacency matrix. what do you get on the trace of A_G^2? a diag. element of A_G^2 is computed $a^2_{ij} = \sum_{j=1}^n a_{ij} \cdot a_{ji}$. each product is 1 when there is an edge between i, j. therefore a_{ij} is the degree of the nodes ($=$ thus case of i). therefore $\mathrm{Tr}(A_G^2) = \sum_{i=1}^n \deg(i) = 2|\mathcal{E}|$

6. NUMBER THEORY

1. 7 pirates, 1 monkey, ≤ 250 coconut ... how many coconuts receives every surviving pirate? use chinese rem. theorem (→ 3.)
3. $\forall\forall$ $\forall$ primes p and $\forall a, b \in \mathbb{Z}$: $(a+b)^p \equiv_p a^p + b^p$. from the 4.6 (binomial coefficient) is $(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k$. Show that $\binom{p}{k}$ is divisible by p for $k \in \{1, \dots, p-1\}$. $\binom{p}{k} = \frac{p!}{(p-k)!k!}$. Numerator contains factor p, denominator is not divisible by p (since all smaller), therefore not divisible (lem 6.6). since $\binom{p}{k} \in \mathbb{N}$, it is divisible by p.
2. $\forall\forall$ $a, b, c, d, m \in \mathbb{Z}$ int $m \geq 1$, from $a \equiv_m b$ and $c \equiv_m d$ follows $ac \equiv_m bd$. from $a \equiv_m b$ and $c \equiv_m d$ follows $\exists s, t \in \mathbb{Z}$: $a - b = ms$, $c - d = mt \to a = ms + b$, $c = mt + d$. therefore $ac = (ms+b)(mt+d) = m^2st + mst + mtb + bd = m \cdot bd$. for $(a+c) \equiv_m (b+d) \Rightarrow m | (a-b)$, $m | (c-d)$. Hence m also divides $(a-b)+(c-d) = (a+c)-(b+d)$ which is definition of $a+c \equiv_m b+d$
4. $\forall\forall$ $\forall a, b \in \mathbb{Z}$ and $m, n \geq 1$ with $\gcd(n, m) = 1$ holds $a \equiv_{mn} b \Leftrightarrow a \equiv_m b \wedge a \equiv_n b$
"⇒" from $a \equiv_{mn} b$ follows $\exists k \in \mathbb{Z}$: $a - b = k(mn)$, therefore also $a - b = n(km) = m(kn)$
"⇐" consider gleichung system $x \equiv_n Rn(b) \wedge x \equiv_m Rm(b)$. from lem 6.16 is $a \equiv_n b \wedge a \equiv_m b \Leftrightarrow a \equiv_n Rn(b) \wedge a \equiv_m Rm(b)$, where $x = a$ is a solution. Also $x = b$ is a solution. since $\gcd(m,n) = 1$, with the CRT (chinese) that solutions for x are congruent modulo mn. therefore $a \equiv_{mn} b$.
$\forall\forall$ 6 | $(n^3 + 5n)$ $\forall n \in \mathbb{N}$. after exercise 3, it's enough to show that $n(n^2+5) \equiv_2 0$ and $n(n^2+5) \equiv_3 0$. n is either even or odd. therefore is $n(n^2+5)$ always even ($\equiv_2 0$). for the second, distinguish 3 cases: $n = 3k$, $3k+1$, $3k+2$. compute the latter 2 and prove $\equiv_3 0$
5. ▷ a, b, c three relatively prime integers. for $n = ab$, $u = ac$ we have for $0 < q_1 \leq n$, $0 < q_2 < m$: $x \equiv_n q_1$, $x \equiv_m q_2$. How many solutions $0 \leq x < mn$ there are, depending on a, b, c, q_1, q_2?
since mn, nm are not relatively prime, we can't use the CRT. we can change the equations. from exercise 4) if we set equivalent equations ① $x \equiv_a q_1$ ② $x \equiv_b q_1$ ③ $x \equiv_a q_2$ ④ $x \equiv_b q_2$ if $q_1 \neq q_2$ there is no solution. otherwise ③ equivalent to ①, we can remove it. 6.16 lem: we get eq. equations ⑤ $x \equiv_a Ra(q_1)$ ⑥ $x \equiv_b Rb(q_1)$ ⑦ $x \equiv_c Rc(q_2)$. since a, b, c relatively, now the CRT can give us an unique solution x_0 in interval $[0, abc[$. general form of solutions is $x_0 + h(abc)$, $h \in \mathbb{N}$. since $mn = a^2bc$, there are exactly a solutions in interval $[0, mn[$
6. Diffiehellman: Alice chooses x_A from $\{0, \dots, p-2\}$. if $x_A = 0$ she sends $q_A = R(g^0) = 1$ and $k_{AB} = Rp(q_B^0) = 1$. should she choose from $\{1, \dots, p-2\}$? No. for every fix x_A there is the same problem. Attacker can check if $q_A = Rp(g^{x_A})$. Is this true, he can compute k_{AB} (since p, q_B, x_A we known). $x_A = 0$ is not much different from other possibilities thus is no problem for the protocol security, since each fix value for x_A (for big p) has extremely small possibility of being chosen. Therefore will the attacker have no success in a great probability.

7. ALGEBRA

1. ▷ G grp. Show or widersprech: $\forall$ subgroups $H_1, H_2 \leq G$ is $H_1 \cup H_2$ subgroup of G. False. proof with counterexample. consider $G = \langle \mathbb{Z}_6, \oplus \rangle$, $H_1 = \{0,3\}$, $H_2 = \{0,2,4\}$. $\{2,3\} \subseteq H_1 \cup H_2$, but $2+3 = 5 \notin H_1 \cup H_2$. therefore union of subgroups is not necessarily a subgroup as well.
2. $\forall$ finite cyclic groups $G_1 = \langle g_1 \rangle$, $G_2 = \langle g_2 \rangle$ holds $G_1 \times G_2 = \langle (g_1, g_2) \rangle$. False. proof: consider $G_1 \times G_2 = \langle \mathbb{Z}_3^*, \cdot \rangle \times \langle 1 \rangle$. Now $\langle (g_1^i, g_2^j) \rangle = \{(g_1^n, g_2^n) \mid n \in \mathbb{Z}\}$. But, for example, $(0,1)$ is not included. Since it is part of $G_1 \times G_2$, our belonging is wrong.
3. $\forall\forall$ all subgroups of $\mathbb{Z}_6^*$ are cyclic. proof: only possibilities of subsets of $\mathbb{Z}_6^* = \{1,5\}$ are $\{1\}, \{5\}, \{1,5\}$. $\langle \{1\}, \cdot, ^{-1}, 1 \rangle$ is trivial cyclic group (show 3 properties, that it reaches all elements of cyclic generated group → therefore equal). $\langle \{5\}, \cdot, ^{-1}, 1 \rangle$ is no group ($5^2 \neq 1$ is not contained). $\langle \mathbb{Z}_6^*, \cdot, ^{-1}, 1 \rangle$ is a group (4th 7.13 and also cyclic (7th 7.15).
4. ▷ $a(x)$ polynome, degree 4 in $GF(7)[x]$ with double NST $x = 2$. $a(3) = 2$, $a(4) = 3$, $a(6) = 5$. find $a(0)$
since $x = 2$ double NST, $a(x) = (x-2)^2 b(x)$ with $\deg(b(x)) = 2$. We know $a(3) = 2 = (3-2)^2 b(3)$, $b(3) = 2$, $a(4) = \dots$, $a(6) = \dots$ It follows for $b(x)$ that $b(3) = 2$, $b(4) = 3 \cdot 4^{-1} = 6$, $b(6) = 5 \cdot 2^{-1} = 6$. Use Lagrange interpolation formula to find $b(x)$ (lem 7.34): $b(x) = 2\frac{(x-4)(x-6)}{(3-4)(3-6)} + 6\frac{(x-3)(x-6)}{(4-3)(4-6)} + 6\frac{(x-3)(x-4)}{(6-3)(6-4)} = 3(x+3)(x+1) + 4 \cdot (x+4)(x+1) + (x+4)(x+3) = x^2 + 4x + 2$
It follows $a(x) = (x-2)^2(x^2+4x+2) = x^4 + 4x^3 + x + 1$, $a(0) = 1$
5. count all irreducible pol. of deg 4 over $GF(2)$ (aufzählen = last). use your list. We show we are right by using all reducible pol of deg 4. $p(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ is reducible if $a_0 = 0$ (lem 7.29), since $x | p(x)$ would hold. $(x+1) | p(x)$ when $-1 = 1$ NST of $p(x)$. this is the case when $a_3 + a_2 + a_1 = 0$, which we can exclude. We have now excluded all polynomes divisible by pol of degree 1. we still need to check those with degree 2. thus is only $1 + x + x^2 \to 12 = x^4 + x^2 + 1$. (all others of deg 2 are divisible by deg 1 → no need to check again). we now remain with the 3 listed in the beginning (not divisible by deg 1 or 2 → irreducible)
6. ▷ F finite field. $\forall\forall$ $\exists$ polynom $a(x) \in F[x]$, not const, without NST in F. ▷ $|F| = n$. we build $a(x) = (x+a_n)(x+a_{n-1}) \dots (x+a_1) + 1$ with $a_i \in F$, $a_i \neq a_j$ for $i \neq j$. With lem 7.31 it follows that $a(x)$ doesn't have any NST in F.
7. ▷ R commutative ring with at least 2 elem $r \in R$. $\forall\forall$: $r \in R^* \Leftrightarrow \forall s \in R \; \exists t \in R: s = rt$
"⇒" to show this direction: ▷ $r \in R^*$. from def of R^*, is r a unit, and therefore invertable. d.h. $\exists u \in R: ru = 1$. for any $s \in R$ holds $s \cdot 1 \cdot s = r \cdot u \cdot s$. with $t = us \in R$ we have $s = rt$. "⇐" ▷ $s = 1$. from assumption $\forall s \in R \; \exists t \in R: s = rt$ there is $t \in R$ with $rt = 1$. t is by def inverse of r. So r is unit, therefore $r \in R^*$
8. ▷ $<G; \cdot, ^{-1}, 1>$, $<H, *, ^\wedge, e>$ groups. $\phi: G \to H$ homomorphism and let $g_0 \in \phi^{-1}(\{e\})$. $\forall\forall$ $\forall g \in G$ $g \cdot g_0 \cdot g^{-1} \in \phi^{-1}(\{e\})$. ▷ G belieby. $\forall\forall$ $g \cdot g_0 \cdot g^{-1} \in \phi^{-1}(\{e\}) \Leftrightarrow \phi(g \cdot g_0 \cdot g^{-1}) \in \{e\} \Leftrightarrow \phi(g \cdot g_0 \cdot g^{-1}) = e$
we have $\phi(g \cdot g_0 \cdot g^{-1}) = \phi(g) * \phi(g_0) * \phi(g^{-1}) = \phi(g) * e * \phi(g^{-1}) = \phi(g) * \phi(g^{-1}) = \phi(g) * \phi(g)^\wedge = e$ as wanted
9. decompose $a(4) := x^4 + x^3 + x^2 + (x+1)q + r \in GF(2)[x]$ in irreducible factors. $a, 1, x, x+1$ are all values q can assume. for tabella $\frac{q \mid 0 \mid 1 \mid x \mid x+1}{r \mid \dots}$ only NST $q = x$. we get $a(4) = (q+x) = x^4 + q + 1$ then we put $a, 1, x, x+1$ in this and get: $0 \to 1$, $1 \to x$, $x \to x^4$, $x+1 \to 1$. since no NST, it can't be divided any further (irreducible), and decomposition is $(x+4)(x^3 + x^2 + q + 1)$